Přírodovědecká fakulta Masarykovy Univerzity
Katedra Algebry a Geometrie

Univerzální slova v grupách a pologrupách

Ondřej Klíma

Brno, duben 1998

Chtěl bych poděkovat doc. Liboru Polákovi za cenné náměty, rady a připomínky, které mi pomohly při psaní této práce.

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a použil jsem pouze uvedené literatury.

Obsah

Úvod

Problematika, kterou se v této práci budeme zabývat, se dotýká základního problému algebry, a to řešení rovnic. Budeme se snažit říci něco málo o řešení rovnic v grupách a pologrupách.

Při studiu rovnic v grupách lze jít mnoha směry. Některé výsledky se týkají například řešení rovnic v rozšíření grup: jisté typy rovnic, s parametry z G, mají řešení v grupě H, která obsahuje jako podgrupu grupu G.

My se budeme ubírat jiným směrem. Předně se budeme zabývat rovnicemi ve speciálním tvaru, v kterých na jedné straně stojí proměnné a na druhé parametr. Budeme se zajímat, zda taková rovnice má či nemá řešení. Základním pojmem pro nás bude univerzální slovo. Slovo $w = w(x_1, \ldots, x_r)$ nazveme univerzální, pokud rovnice $w = s$ bude mít řešení pro libovolný prvek s dané grupy či pologrupy.

V největší míře se budeme zajímat o grupy permutací a monoidy transformací. Budeme se snažit pro takové grupy a pologrupy rozhodnout, zda je v nich dané slovo univerzální. Význam tohoto pozorování je nasnadě. Bude-li slovo univerzální, můžeme pak psát libovolnou transformaci v daném tvaru. Potřeba vědět, zda transformaci lze psát v předepsaném tvaru, byla počátečním impulsem, který vedl k rozvoji teorie univerzálních slov v šedesátých letech.

Některé výsledky, které v práci zmíníme, a které patří do této oblasti, jsou staršího data. Například O. Ore (1951) ukázal, že libovolnou permutaci nekonečné množiny, lze psát jako komutátor. Mohutné zobecnění, a to že v nekonečných permutačních grupách jsou všechna slova, s vyjímkou mocnin, univerzální, pak dokázal R. C. Lyndon (1990).

Pro transformace podobný velký výsledek neexistuje. Přesto bylo dokázáno mnoho netriviálních tvrzení, které se dotýkají dvou velmi zajímavých , a možná také odvážných hypotéz. Ty zformuloval D. M. Silberger v roce 1973, a doposud se je nepodařilo dokázat ani vyvrátit.

Další pojem, se kterým se v práci setkáme je pojem verbální úplnosti. Grupa se nazývá verbálně úplná, pokud v ní jsou univerzální všechna slova. Z výsledků teorie verbálně úplných grup v této práci zmíníme pouze fakt, který se vztahuje k permutačním grupám.

Text je rozdělen do pěti kapitol.

V kapitole první zavedeme základní pojmy.

V druhé kapitole budeme univerzální slova studovat z hlediska univerzální algebry. Taktéž zde uvedeme několik jednoduchých pozorování pro grupy a pologrupy.

Předmět našeho zájmu, a to grupy permutací a monoidy transformací, představíme v kapitole třetí. V této kapitole uvedeme již zmíněné hypotézy a pokusíme se naznačit souvislosti, které se jich týkají.

Čtvrtá kapitola obsahuje důkaz tvrzení o verbálně úplných faktorgrupách nekonečných permutačních grup. Také zde uvedeme jednoduchá tvrzení o verbálně úplných pologrupách.

Poslední kapitola zkoumá slova tvaru $x^n y^m$ v grupách permutací a monoidech transformací. Je zde dokázána věta charakterizující slova $x^n y^m$, která jsou univerzální ve všech monoidech transformací. V druhé části této kapitoly pak ukážeme, že každé slovo $x^n y^m$, které je univerzální v nějaké konečné grupě permutací, je univerzální ve všech monoidech transformací na dostatečně velké konečné množině.

Aktualizace 1

Po přečtení posudků, jsem opravil několik drobných přepisů a několik důkazů. Rád bych zde naznačil, jak se liší zveřejněná aktualizovaná verze od původní verze diplomové práce. Nemá smysl uvádět všechny překlepy apod., a proto se omezím pouze na okomentování větších úprav.

1. Důkaz lemmatu 5.3 jsem poněkud upravil podle návrhu dr. Kaďourka.

2. Lemma 5.6. je zcela nové. Při psaní DP jsem se domníval, že toto tvrzení je jednoduchým důsledkem předchozích úvah, což nebyla pravda, jak upozornil dr. Kaďourek ve svém posudku.

Děkuji touto cestou dr. Kaďourkovi za cenné přpomínky obsažené v posudku, které se promítli do této aktualizace.

Kapitola 1

Označení a základní definice

Budeme pracovat s následujícím označením.
$\mathbb{N}$ je množina všech přirozených čísel, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{N}_\infty = \mathbb{N} \cup \{\aleph_0\}$.
$\mathbb{Z}$ je množina všech celých čísel.
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou množiny všech racionálních, reálných a komplexních čísel.
$\mathbb{Q}^+$, $\mathbb{R}^+$ množiny všech kladných racionálních a reálných čísel.
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Buď $\mathcal{V}$ varieta algeber. Označme $F_\mathcal{V}$ volnou algebru této variety s množinou generátorů $\{x, y, \dots\}$. Buď $w \in F_\mathcal{V}$ slovo a $A \in \mathcal{V}$ algebra. Řekneme, že w *reprezentuje* $a \in A$, jestliže existuje homomorfismus $\alpha : F_\mathcal{V} \to A$ tak, že $\alpha(w) = a$. Slovo w je *univerzální* v A pokud reprezentuje všechny prvky $a \in A$.

Jinak řečeno: slovo $w = w(x_1, \dots, x_r)$ je univerzální v A, pokud pro libovolné $a \in A$ existuje posloupnost $a_1, \dots, a_r$ prvků z A taková, že $a = w(a_1, \dots, a_r)$. Nebo-li rovnice $a = w(x_1, \dots, x_r)$ má řešení v A.

Příklady.
1) Slovo x je univerzální v libovolné algebře.
2) Ve varietě všech pologrup je slovo x^3 univerzální v $(\mathbb{Z}_k, +)$ pro $3 \nmid k$ a není univerzální v $(\mathbb{Z}_3, +)$.
3) Ve varietě všech svazů je libovolné slovo univerzální v libovolném svazu, protože pro libovolné $w = w(x_1, \dots, x_r)$ platí $w(a, \dots, a) = a$.
4) Varieta všech okruhů. Libovolný polynom lichého stupně (tj. slovo v jedné proměnné) je univerzální v $\mathbb{R}$. Naopak polynomy sudého stupně nejsou univerzální v $\mathbb{R}$.

Kapitola 2

Univerzalita a třídy struktur

Nás budou nejvíce zajímat grupy a pologrupy, avšak dříve než přistoupíme k jejich studiu, pokusme se zformulovat několik poznatků o univerzálních slovech, které platí pro libovolné algebry.

Základní vlastnosti univerzálních slov

Věta 1.
Pokud máme dvě slova v, w taková, že v vznikne z w při vhodné substituci a v je univerzální v algebře A, pak w je taktéž univerzální v A.
Důkaz:
Podmínka o substituci požaduje existenci homomorfismu $\varphi : F_{\mathcal{V}} \to F_{\mathcal{V}}$ splňujícího $\varphi(w) = v$. Je-li v univerzální v A znamená to, že pro libovolné $a \in A$ existuje $\alpha : F_{\mathcal{V}} \to A$ splňující $\alpha(v) = a$. Pro w máme tedy homomorfismus $\alpha \circ \varphi : F_{\mathcal{V}} \to A$, který umožňuje reprezentaci prvku $a \in A$. $\square$

Důsledek 2.
Nechť φ je automorfismus $F_{\mathcal{V}}$. Slovo w je univerzální v algebře A právě tehdy, když $\varphi(w)$ je univerzální v A.

Příkladem automorfismu $F_{\mathcal{V}}$ je automorfismus indukovaný bijekcí na množině generátorů. Budeme-li v dalším říkat, že nějaké slovo w je univerzální, budeme vědět, že jsou univerzální taktéž slova, která lze z w získat přejmenováním proměnných.

Poznamenejme, že pro některé variety jiné automorfismy neexistují. To je případ pologrup. Naopak pro varietu grup máme i jiné automorfismy volné grupy, např. vnitřní automorfismy.

Věta 3.
Buď $\beta : A \to B$ surjektivní homomorfismus algeber, pak slova univerzální v A jsou taktéž univerzální v B.
Důkaz:
Nechť slovo w je univerzální v A. Chceme ukázat, že je univerzální i v B. Buď tedy $b \in B$ libovolný prvek, pak existuje $a \in A$ takový, že $\beta(a) = b$. Protože w reprezentuje a, máme zaručenu existenci $\alpha : F_{\mathcal{V}} \to A$ s vlastností $\alpha(w) = a$. Odtud $(\beta \circ \alpha)(w) = b$, čímž jsme získali homomorfismus $\beta \circ \alpha : F_{\mathcal{V}} \to B$, který umožňuje reprezentaci prvku b slovem w. $\square$

Odtud a z faktu, že libovolná algebra je kvocientem volné algebry plyne, že slovo w je univerzální ve všech algebrách dané variety právě tehdy, když je univerzální ve volných algebrách (s libovolně mnoha generátory).

Označme nyní $\mathcal{U}(w)$ třídu všech algeber dané variety v nichž je slovo w univerzální. Důsledek 2 lze v tomto kontextu formulovat tak, že pro φ, automorfismus $F_{\mathcal{V}}$, platí

$$\mathcal{U}(w) = \mathcal{U}(\varphi(w)).$$

Podobně pro množinu slov W označme $\mathcal{U}(W)$ třídu algeber v nichž jsou univerzální všechna slova z W. Definice univerzálního slova lze interpretovat tímto způsobem: $w = w(x_1, \ldots, x_r)$ je univerzální v algebře A, jestliže v A platí sentence

$$\phi_w = (\forall\ s)(\exists\ s_1, \ldots, s_r)(s = w(s_1, \ldots, s_r)).$$

To znamená, že třída $\mathcal{U}(W)$ je třída algeber v níž platí množina sentencí $\Phi = \{\phi_w \mid w \in W\}$ a množina sentencí Ψ , které zaručují platnost identit definujících varietu. Takovým třídám říkáme *axiomatické třídy.* V [6] lze nalézt následující charakterizaci axiomatických tříd.

Věta 4.
Třída struktur $\mathcal{T}$ je axiomatická $\iff$ jsou splněny následující dvě podmínky
(i) $\mathcal{T}$ je uzavřena na ultrasoučiny,
(ii) $\mathcal{T}$ je uzavřena na elementární ekvivalenci.

V našem případě však třída $\mathcal{U}(W)$ splňuje víc. Již jsme dokázali, že $\mathcal{U}(W)$ je uzavřena na homomorfní obrazy. Snadno se také vidí, že je uzavřena na součiny. Tyto dvě vlastnosti jsou silnější než podmínka (i) v předchozí větě, protože ultrasoučin je kvocientem součinu. K tomu, aby třída byla varietou je ještě třeba, aby byla uzavřena na podalgebry. To však obecně neplatí. Poznamenejme, že třída $\mathcal{U}(W)$ je taktéž uzavřena na sjednocení řetězců.

Příklady.
1) Ve varietě grup je slovo x^3 univerzální v $(\mathbb{R}^*, \cdot)$, ale není univerzální v $(\mathbb{Q}^*, \cdot)$.
2) Varieta komutativních grup $\mathcal{A}$ je uzavřena na homomorfní obrazy i součiny. Ve větě 5 ukážeme, že pokud je slovo univerzální v $\mathbb{Z}$, potom je univerzální ve všech grupách. Je-li tedy W množina slov, která jsou univerzální ve všech grupách třídy $\mathcal{A}$, potom $\mathcal{U}(W)$ je varieta všech grup. $\mathcal{A}$ tedy není tvaru $\mathcal{U}(W)$.
3) V pologrupách platí $\mathcal{U}(x^2) = \mathcal{U}(x^4)$.

Slova univerzální ve všech pologrupách a grupách

Pokusme se nyní zodpovědět otázku, jak vypadají slova, která jsou univerzální ve všech pologrupách, monoidech a grupách. Jistou podmínku jsme již zmínili, můžeme však jít ještě dále.

Příklady.
1) Jediné slovo, univerzální ve všech pologrupách, je x, poněvadž to jediné je univerzální v pologrupách s konstantním násobením – tj. pologrupách s význačným prvkem 0, přičemž $ab = 0$ pro libovolné a, b. Poznamenejme, že tyto pologrupy tvoří varietu, která je definována identitou $xy = zt$.
2) Vezmeme-li pologrupu z předchozího bodu a doplníme ji neutrálním prvkem na monoid, vidíme, že slovo $w = w(x_1, \ldots, x_r)$ je v takovém monoidu univerzální právě tehdy, když obsahuje některou proměnnou právě v jednom výskytu. Tato podmínka je již postačující k tomu, aby w bylo univerzální ve všech monoidech.
3) (Čtenáři, který není obeznámen s pojmem inverzní pologrupa, doporučujeme vrátit se k tomuto příkladu až po přečtení celé kapitoly.)
Uvažme inverzní pologrupu s násobením zadaným následující tabulkou.

·	0	a	a’	aa’	a’a
0	0	0	0	0	0
a	0	0	aa’	0	a
a’	0	a’a	0	a’	0
aa’	0	a	0	aa’	0
a’a	0	0	a’	0	a’a

Tato pologrupa se označuje B_2 a říká se jí pětiprvková Brandtova pologrupa. V kapitole 3 ji popíšeme ještě jiným způsobem. B_2 nám umožní testovat, zda je slovo univerzální ve všech inverzních pologrupách. Nechť slovo w reprezentuje prvek a v B_2, tedy $a = w(a_1, \ldots, a_r)$ pro vhodná $a_1, \ldots, a_r \in B_2$. Pro libovolnou inverzní pologrupu S a libovolný prvek $s \in S$

pak můžeme psát $s = w(s_1, \dots, s_r)$, kde pro $i = 1, \dots, r$ klademe

$$s_i = \begin{cases} s & \text{pokud} \quad a_i = a \\ s' & \text{pokud} \quad a_i = a' \\ ss' & \text{pokud} \quad a_i = aa' \\ s's & \text{pokud} \quad a_i = a'a. \end{cases}$$

Nyní popíšeme, podobně jako v předchozím příkladě, slova univerzální ve všech grupách. Označme nejdříve $\sharp_x(w)$ součet mocnin u x ve slově w. Precizněji, je-li $w = w(x_1, \dots, x_r)$ pak $\sharp_{x_i}(w)$ označuje takové $k \in \mathbb{Z}$, pro něž platí

$$w(1, \dots, 1, x_i, 1, \dots, 1) = x_i^k.$$

Nyní můžeme zformulovat následující větu.

Věta 5.
Slovo $w(x_1, \dots, x_r)$ je univerzální ve všech grupách $\iff$ čísla $\sharp_{x_i}(w)$, kde $i = 1, \dots, r$, jsou nesoudělná.
Důkaz:
$\Longleftarrow$: Z Bezoutovy věty máme zaručenu existenci $n_1, \dots, n_r \in \mathbb{Z}$ takových, že

$$\sum_{i=1}^{r} n_i \cdot \sharp_{x_i}(w) = 1.$$

Stačí tedy pro libovolné $g \in G$ volit $x_i = g^{n_i}$.
$\Longrightarrow$: Pokud jsou čísla $\sharp_{x_i}(w)$ soudělná, pak existuje $1 < n \in \mathbb{N}$ takové, že $n \mid \sharp_{x_i}(w)$. Pak ale w nemůže být univerzální v $(\mathbb{Z}_n, +)$, neboť pro libovolná $g_1, \dots, g_r \in \mathbb{Z}_n$ platí

$$w(g_1, \dots, g_r) = \sum_{i=1}^{r} \sharp_{x_i}(w) \cdot g_i = n \cdot \sum_{i=1}^{r} \frac{\sharp_{x_i}(w)}{n} \cdot g_i = 0. \quad \square$$

Poznamenejme, že autoři článku [4] zformulovali předchozí větu do ekvivalence s podmínkou, že w je univerzální v $(\mathbb{Z}, +)$. To plyne z předchozího a věty 3, neboť $(\mathbb{Z}_n, +)$ je kvocientem $(\mathbb{Z}, +)$.

Duální slova

Duálním slovem k slovu w nazýváme slovo, které vznikne budeme-li číst slovo w odzadu. Označujeme jej $\overline{w}$. V následujícím ukážeme, že v jistých varietách platí $\mathcal{U}(w) = \mathcal{U}(\overline{w})$.

Grupy mají přirozené zobecnění, kterým jsou inverzní pologrupy. Řekneme, že pologrupa S je *inverzní* pokud

$$\forall\ a \in S\ \exists!\ b \in S : aba = a,\ bab = b.$$

Takový prvek b se označuje zpravidla a^{-1} nebo a' a nazývá se inverze. Mnohé vlastnosti inverzních pologrup jsou popsány v [7] (Hlava V). Nás bude pro tuto chvíli pouze zajímat, že platí následující vztahy: (Viz [7](str.131).)

$$(a^{-1})^{-1} = a, \quad (ab)^{-1} = b^{-1}a^{-1}.$$

Unárním pologrupám, kde platí tyto dva vztahy, říkáme *involutární*, unární operaci obvykle značíme $'$. Mezi involutární pologrupy patří také $*-$regulární pologrupy, v kterých navíc platí

$$aa^{-1}a = a.$$

Díky identitám

$$(x^{-1})^{-1} = x, \quad (xy)^{-1} = y^{-1}x^{-1}$$

platí následující věta, kterou zformulujeme pro inverzní pologrupy, ale která platí taktéž pro pologrupy involutární a $*-$regulární.

Věta 6.
Buď S libovolná inverzní pologrupa. Slovo w je univerzální v S právě tehdy, když $\overline{w}$ je univerzální v S.
Důkaz:
Stačí když ukážeme jednu implikaci, neboť druhá potom bude plynout z faktu, že $\overline{\overline{w}} = w$. Buď $w = w(x_1, \ldots, x_r)$ univerzální v S a $s \in S$ libovolný prvek. Pak $s^{-1} \in S$ a lze tedy psát $s^{-1} = w(s_1, \ldots, s_r)$, pro vhodné $s_1, \ldots, s_r \in S$. Odtud

$$s = [w(s_1, \ldots, s_r)]^{-1} = \overline{w}(s_1^{-1}, \ldots, s_r^{-1}).$$

Proto umíme slovem $\overline{w}$ reprezentovat libovolný prvek s. $\square$

Důsledek 7.
Buď G libovolná grupa. Slovo w je univerzální v G právě tehdy, když $\overline{w}$ je univerzální v G.

Kapitola 3

Univerzalita v grupách permutací a příbuzných strukturách

V této práci budeme především studovat speciální třídu monoidů a grup.

Permutace, transformace

Zavedeme následující označení:

$$\begin{array}{lcl} PT(X) & = & \{s \mid s : Y \to X, Y \subseteq X\}, \\ I(X) & = & \{s \in PT(X) \mid s \text{ injekce}\}, \\ T(X) & = & \{s \mid s : X \to X\}, \\ S(X) & = & \{s \in T(X) \mid s \text{ bijekce}\}. \end{array}$$

Platí tedy $S(X) \subseteq T(X) \subseteq PT(X)$ a také $S(X) \subseteq I(X) \subseteq PT(X)$. Pro konečné X navíc platí $S(X) = I(X) \cap T(X)$.

Prvkům z množiny $T(X)$ říkáme transformace, $PT(X)$ parciální transformace, $I(X)$ prosté parciální transformace, či zkráceně prosté transformace, a prvkům z $S(X)$ permutace.

Pro $s : Y \to X$ označujeme

$$\begin{array}{lcl} Dom(s) & = & Y, \\ Im(s) & = & \{e \in X \mid \exists f \in Y : s(f) = e\}, \\ Wrld(s) & = & Dom(s) \cup Im(s). \end{array}$$

Pro $s \in S(X)$ označujeme $supp(s) = \{e \in X \mid s(e) \neq e\}$.
Permutace $a, b \in S(X)$ jsou *disjunktní*, jestliže $supp(a) \cap supp(b) = \emptyset$.

Společně s operací skládání zobrazení tvoří výše popsané množiny monoidy. V případě $I(X)$ dokonce inverzní pologrupu a v případě $S(X)$ grupu.

Pro konečné X budeme někdy tyto monoidy označovat $PT(k)$, $I(k)$, $T(k)$ a $S(k)$ kde $k \in \mathbb{N}$, $k = |X|$. Navíc označme $A(k) \subseteq S(k)$ podgrupu všech sudých permutací. Grupám $A(k)$ říkáme *alternující*.

Pro nekonečná X označme $S^0(X)$, $A(X)$ normální podgrupy $S(X)$ takovéto:

$$\begin{array}{rcl} S^0(X) & = & \{s \in S(X) \mid supp(s) \text{ konečná } \}, \\ A(X) & = & \{s \in S^0(X) \mid s\,|_{supp(s)} \text{ sudá } \}. \end{array}$$

O těchto podgrupách řekneme více v kapitole 4.

Tyto struktury hrají důležitou roli v teorii grup a pologrup, neboť reprezentují všechny pologrupy jistých vlastností. Pro grupy máme Cayleyho větu, která říká, že pro libovolnou grupu G existuje množina X a injektivní homomorfismus $\alpha : G \hookrightarrow S(X)$. Podobně pro každý monoid M existuje množina X a injektivní homomorfismus $\alpha : M \hookrightarrow T(X)$. Pologrupu, která není monoidem lze přidáním neutrálního prvku rozšířit na monoid. Tím pádem umíme i libovolnou pologrupu vložit do vhodné $T(X)$. Stejným způsobem reprezentují $I(X)$ inverzní pologrupy: v [7] (str 133–136) lze nalézt důkaz tvrzení, že pro každou inverzní pologrupu S existuje množina X a injektivní homomorfismus $\alpha : S \hookrightarrow I(X)$. Ve všech třech uvedených případech lze za X brát nosnou množinu příslušné algebry.

Disjunktní rozklady

Podívejme se nyní jak vypadají prvky v našich monoidech. Na prvky $T(X)$ lze nahlížet, jako na unární algebry s nosnou množinou X.

Další možností je představit si parciální transformaci jako orientovaný graf, v němž z každého vrcholu vychází nejvýše jedna hrana. Takový graf se nám potom rozpadne na souvislé komponenty. Tato představa nám dobře poslouží k rozkládání prostých transformací na disjunktní souvislé prosté transformace. Transformaci $s \in PT(X)$ nazveme *souvislou*, jestliže

$$\forall\, e, f \in X\ \exists\, n, m \in \mathbb{N}_0 : s^n(e) = s^m(f).$$

Je dobře známo, že prvek v konečné grupě $S(k)$ lze rozložit na součin disjunktních cyklů. Pro nekonečná $S(X)$ lze stejně rozkládat libovolný prvek, avšak v rozkladu se může navíc vyskytnout nekonečný had. *Nekonečný had* je permutace $s \in S(X)$ taková, že $s(e_i) = e_{i+1}$, kde $e_i \in X$ různé a i probíhá množinu $\mathbb{Z}$. Na obrázku je příklad nekonečného hada, přičtení 1 na $\mathbb{Z}$.

$$\cdots \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

Podobně prvek z $I(k)$ je součin disjunktních cyklů a konečných hadů. *Hadem* rozumíme zobrazení $s \in I(k)$ takové, že $s(e_i) = e_{i+1}$, kde $e_i \in X$ různé a $i = 1, \ldots, l-1$, přičemž $l(\leq k)$ pak nazýváme *délkou hada*. Na následujícím obrázku je had délky 4.

$$1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4$$

Pro nekonečné $I(X)$ lze každý prvek psát jako součin disjunktních cyklů, hadů, nekonečných hadů, nekončících a nezačínajících hadů. *Nekončící had* je zobrazení $s \in I(X)$ takové, že $s(e_i) = e_{i+1}$, kde $e_i \in X$ různé a i probíhá množinu $\mathbb{N}$. *Nezačínající had* je zobrazení $s \in I(X)$ takové, že $s(e_{i+1}) = e_i$, kde $e_i \in X$ různé a i probíhá množinu $\mathbb{N}$. Poznamenejme, že nezačínající had je inverzí nekončícího hada. Na následujícím obrázku jsou hadi: přičtení a odečtení 1 na $\mathbb{N}$.

$$1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \quad \cdots$$

$$1 \longleftarrow 2 \longleftarrow 3 \longleftarrow \quad \cdots$$

Pro $s \in S(X)$ zavádíme

$$\widetilde{s} : \mathbb{N}_\infty \to \{c \,|\, 0 \le c \le |X|\},$$

kde $\widetilde{s}(n)$ je mohutnost množiny všech cyklů délky n pro $n \in \mathbb{N}$ a $\widetilde{s}(\aleph_0)$ je mohutnost množiny všech nekonečných hadů v rozkladu s.
O dvou permutacích $a, b \in S(X)$ řekneme, že jsou *konjugované*, jestliže

$$\exists\; c \in S(X) : a = c^{-1}bc$$

a píšeme $a \sim b$. Konjugovanost znamená, že a a b se liší pouze přejmenováním prvků množiny X. Přesnější popis dává následující jednoduché lemma.

Lemma 1.
Dvě permutace $a, b \in S(X)$ jsou konjugované právě tehdy, když $\widetilde{a} = \widetilde{b}$.

Příklady.
1) Rovnice $x^2 = s$ má řešení v $S(k)$ právě tehdy, když $\widetilde{s}(2n)$ je sudé pro každé $n \in \mathbb{N}$.

2) Obecněji, rovnice $x^m = s$ v $S(k)$. Nechť $m = p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r} \in \mathbb{N}$, kde $p_1 < \cdots < p_r$ jsou prvočísla a $\varepsilon_1, \dots, \varepsilon_r \in \mathbb{N}$. Předpokládejme, že a je řešení rovnice, tzn. $a^m = s$. Nechť v rozkladu s na disjunktní cykly je nějaký cyklus délky n, pak musel vzniknout z cyklu délky $l \cdot n$ v a, přičemž umocnění dalo l cyklů délky n. Předpokládejme, že pro některé prvočíslo p_i platí $p_i \,|\, n$. Pro toto prvočíslo pak musí taktéž platit $p_i^{\varepsilon_i} \,|\, l$, v opačném případě by totiž umocnění cyklu délky $l \cdot n$ nemohlo dát cyklus délky n. Proto

$$p_i \,|\, n \Longrightarrow p_i^{\varepsilon_i} \,|\, l,$$

tedy

$$p_i \,|\, n \Longrightarrow p_i^{\varepsilon_i} \,|\, \widetilde{s}(n).$$

Celkem: má-li mít rovnice $x^m = s$ řešení, pak musí pro všechna $n \in \mathbb{N}$ platit

$$n.s.d.(m, n^m) \mid \widetilde{s}(n),$$

neboť

$$n.s.d.(m, n^m) = \prod p_i^{\varepsilon_i},$$

kde násobíme přes všechna i pro něž $p_i \mid n$.

3) Slovo x^m je univerzální v $S(k) \iff k < p$ pro všechna prvočísla $p \mid m$.

4) Při řešení rovnice $x^m = s$, kde $s \in S(X)$ (X nekonečná), uvažme nejdříve následující jednoznačný rozklad $s = a \circ b$, kde a, b jsou disjunktní, a obsahuje pouze konečné cykly a b pouze nekonečné. Potom rovnice $x^m = s$ má řešení v $S(X)$ právě tehdy, když rovnice $x^m = a$ má řešení v $S(Dom(a))$ a $m \mid \widetilde{b}(\aleph_0) = \widetilde{s}(\aleph_0)$.

Příklad.
V kapitole 2 jsme slíbili popis B_2. Zde je:

$$B_2 = \{s \in I(2) \mid |Im(s)| \leq 1\}.$$

Implikace tykající se univerzality slov

Přestože obecně neplatí implikace týkající se univerzálnosti slov v podalgebrách, jak jsme konstatovali v kapitole 2, můžeme takové implikace dokázat pro monoidy transformací.

Věta 1.
Pro libovolnou množinu X platí: je-li w univerzální v $PT(X)$, pak je univerzální v $T(X)$.
Důkaz:
Nechť $w = w(x_1, \dots, x_r)$ je univerzální v $PT(X)$ a $s \in T(X) \subseteq PT(X)$ libovolné. Pak existují $a_1, \dots, a_r \in PT(X)$ taková, že $s = w(a_1, \dots, a_r)$. Zvolme $e \in X$ libovolné, ale pevné. Pro $i = 1, \dots, r$ nyní definujme $s_i \in T(X)$ takto:

$$s_i(f) = \begin{cases} a_i(f), & f \in Dom(a_i) \\ e, & f \notin Dom(a_i) \end{cases}$$

Protože

$$\forall\, f \in X : w(s_1, \dots, s_r)(f) = w(a_1, \dots, a_r)(f) = s(f),$$

pro námi definované $s_1, \dots, s_r$ platí

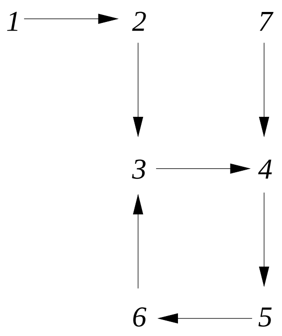
$$w(s_1, \dots, s_r) = w(a_1, \dots, a_r) = s. \;\Box$$

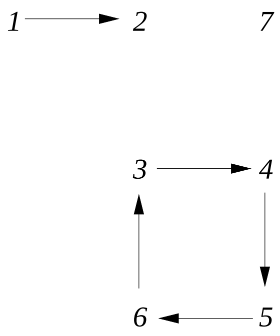
Věta 2.
Pro libovolnou konečnou množinu X platí: je-li w univerzální v $T(X)$, pak je univerzální v $S(X)$.
Důkaz:
Buď $w = w(x_1, \ldots, x_r)$ univerzální v $T(k)$ a $s \in S(k) \subseteq T(k)$, pak existují $s_1, \ldots, s_r \in T(k)$ taková, že $s = w(s_1, \ldots, s_r)$. Stačí ukázat, že $s_i \in S(k)$. Pokud by některé $s_i \notin S(k)$, potom $|Im(s)| \leq |Im(s_i)| < k$ a tedy $s \notin S(k)$. Spor. $\square$

Věta 3.
Pro libovolnou konečnou množinu X platí: je-li w univerzální v $I(X)$, pak je univerzální v $S(X)$.
Důkaz:
Naprosto stejně jako předchozí. $\square$

Předchozí dvě věty platí i pro nekonečné množiny X. Proč tomu tak je bude vysvětleno v kapitole 4, kde se budeme zabývat nekonečnými permutačními grupami. Vztah mezi $PT(X)$ a $I(X)$ je poněkud jiný.

Věta 4. [D. M. Silberger [14] – 1.1.]
1) Slovo w je univerzální ve všech $PT(X) \iff w$ reprezentuje všechny souvislé prosté transformace s v $PT(Wrld(s))$.
2) Buď $l \in \mathbb{N}$ a nechť w reprezentuje všechny souvislé prosté transformace s v $PT(Wrld(s))$ pro něž $|Wrld(s)| \leq l$. Potom je slovo w univerzální v $PT(k)$ pro každé $k \leq l$.
Důkaz:
Pouze naznačíme. Reprezentace libovolného prvku s se provede následujícím způsobem. Nejdříve prvek s „rozstříháme“ na hady s_i, ty reprezentujeme v $PT(Wrld(s_i))$ a nakonec „poslepujeme“. Ilustrujme tento postup na příkladě.

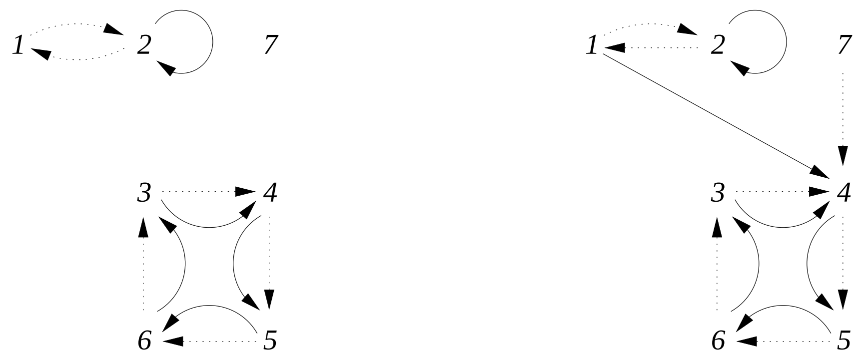




Na prvním obrázku je prvek $s \in PT(7)$, který chceme reprezentovat slovem x^2y^2x. Na druhém je pak prvek $s' \in I(7)$, který vznikl z s odstraněním některých přiřazení. Tento prvek, má-li konstrukce fungovat, musí být uzavřen na některé vzory vzhledem k s. Přesněji: je-li $s \in PT(X)$, potom musí pro $s' \in I(X)$ platit

$$\forall\, e \in Dom(s') : s'(e) = s(e), \quad \forall\, e \in Im(s)\, \exists\, f \in X : s'(f) = e.$$

Poznamenejme, že takových prvků s' může být více. Nyní s' rozepíšeme do tvaru a^2b^2a a to tak, že jednotlivé komponenty disjunktního rozkladu s_i reprezentujeme v $PT(Wrld(s_i))$. V našem příkladě jsou to hadi délky 1 a 2 a cyklus délky 4. Na třetím obrázku je tečkovaně označena transformace a a plnou čarou transformace b pro něž platí $s' = a^2b^2a$. Vzhledem ke konstrukci s' můžeme doplnit transformace tak, abychom dostali původní transformaci s, jak je ukázáno na obrázku čtvrtém.



Tímto způsobem, lze dokázat 2. část tvrzení. Obecný důkaz 1. části využívá axiomu výběru. Pro dané slovo w a prvek $s \in PT(X)$ se uváží všechna možná zúžení s, která jsou uzavřena na některé vzory vzhledem k s. Pro každé takové zúžení se pak vezmou všechny možné reprezentace. Relací rozšířemí se uspořádají všechny reprezentace (reprezentace=homomorfismus $F_{\mathcal{V}} \to PT(X)$, pro reprezentace α, α' definujeme $\alpha \leq \alpha'$ pokud pro libovolné $u \in F_{\mathcal{V}}$ je transformace $\alpha'(u)$ rozšířením $\alpha(u)$). Pomocí axiomu výběru pak budeme mít k dispozici maximální prvek, o kterém se díky metodě „slepování“ dá ukázat, že je reprezentací prvku s. Podrobný důkaz lze nalézt v [14]. $\square$

Měli bychom zdůraznit, že v předchozí větě se souvislé prosté transformace reprezentují v parciálních transformacích a nikoli v prostých parciálních transformacích. Ilustrujme tento rozdíl na příkladu.

Příklad.
Slovo x^2y^2 reprezentuje hada délky $2k$ v $PT(2k)$, nikoli však v $I(2k)$. Pokud by a^2b^2 pro $a, b \in I(2k)$ byl had délky $2k$, potom bychom doplněním a, b na permutace obdrželi cyklus délky $2k$ psaný ve tvaru a^2b^2 pro $a, b \in S(2k)$. To nelze, neboť cyklus délky $2k$ je lichá permutace. Metodou z lemmatu 5.3 lze nalézt $a, b \in P(2k)$ taková, že a^2b^2 je had délky $2k$.

Věta 5.
1) Jestliže je slovo w univerzální v $I(X)$ pro všechna X, pak je univerzální v libovolném $PT(X)$.
2) Jestliže je slovo w univerzální v $I(k)$ pro všechna $k \leq l$, pak je univerzální v $PT(l)$.
Důkaz:
Plyne přímo z předchozí věty. $\square$

Příklad.
Jednoduchou aplikací předchozího důsledku dostaneme například, že libovolné slovo tvaru $(xy)^n x$ je univerzální ve všech $PT(X)$.

Je stále otevřenou otázkou, zda první část věty 4 platí taktéž pro transformace.

Hypotéza. [D. M. Silberger – 1973]
Jestliže je slovo w univerzální v $T(X)$ pro všechna X, pak je univerzální v libovolném $PT(X)$.

Příklad.
V této souvislosti je často uváděn následující příklad. Slovo $w = x^2y^2x$ je univerzální ve všech konečných $T(X)$, není univerzální v $PT(3)$ a není univerzální v $T(\mathbb{N})$. Slovo w totiž nereprezentuje hady délky 3 v $PT(3)$ a taktéž přičtení 1 v $T(\mathbb{N})$. J. R. Isbell [8] ukázal, že libovolný prvek $s \in T(k)$ lze psát ve tvaru $a^n b$, kde n je mocnina prvočísla a b je involuce $(\widetilde{b}(m) = 0 \; \forall \; 2 < m \in \mathbb{N})$. Odtud plyne, že slovo w je univerzální ve všech konečných $T(X)$.

Několik příkladů

Nyní uvedeme několik jednoduchých příkladů slov a určíme zda jsou univerzální v permutačních a alternujících grupách.

Příklady.
1) x^2y^2 není univerzální v $S(k)$.
Důkaz:
Pro libovolné $a, b \in S(k)$ jsou a^2, b^2 sudé permutace, tedy a^2b^2 je sudá permutace.

2) x^2y^2 je univerzální ve všech $A(k)$.
Důkaz:
Buď $s \in A(k)$. V rozkladu na disjunktní cykly jsou jednak cykly liché délky, ty necháme být, a sudé délky, ty upravíme dle následujícího vzoru:

$$(1, 2, \ldots, 2n) = (1, 2, \ldots, 2n-1) \circ (2n-1, 2n).$$

Nyní do a zahrnu všechny cykly liché délky nového rozkladu, a do b všechny cykly délky 2, tedy $s = a \circ b$. V b jsou cykly délky 2, přičemž jejich počet je roven počtu cyklů sudé délky v s a ten je sudý, neboť $s \in A(k)$. Vzhledem k tomu jak jsme postupovali, existuje v každém cyklu délky 2 v b prvek e takový, že $a(e) = e$. Cykly z b zpárujeme, upravíme dle vzoru

$$(1,2)(3,4) = (1,4,3)(1,2,3) \quad \text{kde } 1,3 \notin supp(a)$$

a cyklus $(1,4,3)$ přesuneme do a. Pokud $4 \in supp(a)$, potom v rozkladu a se z nějakého cyklu délky $2l-1$ stane cyklus délky $2l+1$. Nyní se a i b sestávají z cyklů liché délky a ty lze v $A(k)$ odmocnit.

3) x^2y^2 je univerzální v nekonečných $S(X)$.
To konstatovali v [4]. Nebudeme to zde dokazovat, neboť v kapitole 5 bude dokázáno obecnější, že $x^n y^m$ je univerzální v nekonečných $S(X)$.

Následující dva poznatky dokázal O. Ore [12].
4) $[x,y] = x^{-1}y^{-1}xy$ je univerzální v $A(k)$ pro $k \geq 5$.
Důkaz:
Buď $s \in A(k)$. Nejdříve rozepíšeme cykly liché délky z s tímto způsobem:

$$(1,2)(3,4)\dots(2k-1,2k) \circ (2,3)(4,5)\dots(2k-2,2k-1)(2k,2k+1)$$

a cykly sudé délky

$$(1,2)(3,4)\dots(2k-1,2k) \circ (2,3)(4,5)\dots(2k-2,2k-1),$$

nebo

$$(2,3)(4,5)\dots(2k-2,2k-1) \circ (1,2)(3,4)\dots(2k-1,2k).$$

A to tak, že $s = a \circ b$, kde a, b obsahuje stejný počet cyklů délky 2. Pokud je tento počet lichý (tzn. $a, b \notin A(k)$), potom lze psát $s = a \circ (e,f)(e,f) \circ b$, kde $e, f \in X$ vlastností

$$e \in supp(a) \setminus supp(b), \quad f \in supp(b) \setminus supp(a).$$

Tedy $s = a \circ b$, kde $a \sim b$, $a, b \in A(k)$. Protože $a \sim a^{-1}$, lze psát $b = c^{-1}a^{-1}c$, nebo-li $s = [a^{-1}, c]$. Pokud $c \in A(k)$ máme tvrzení dokázáno, pokud ne, rozlišíme dva případy:
i) a obsahuje nějaký cyklus délky 2, např. $(1,2)$, potom můžeme psát

$$s = ac^{-1}(1,2)a^{-1}(1,2)c = a((1,2)c)^{-1}a^{-1}((1,2)c) = [a^{-1}, (1,2)c].$$

ii) v a není žádný cyklus délky 2, pak vzhledem ke konstrukci a je $a = (1,2,3)$ a lze tedy psát

$$s = ac^{-1}(4,5)a^{-1}(4,5)c = a((4,5)c)^{-1}a^{-1}((4,5)c) = [a^{-1}, (4,5)c].$$

5) $[x, y]$ je univerzální v nekonečných $S(X)$.
Nebudeme zde dokazovat, lze nalézt v [12].

Neorámovaná a duální slova v transformacích

Slovo w, které lze psát ve tvaru $w = vuv$ (v neprázdné) nazýváme *orámované*. Slova, která v takovém tvaru psát nelze nazýváme *neorámovaná*.

Věta 6. [J. R. Isbell [8], D. M. Silberger [14] – 3.12.]
Jestiže slovo w je neorámované, pak je univerzální v $T(X)$ i $PT(X)$ pro libovolnou nekonečnou množinu X.
Důkaz:
Buď $s \in PT(X)$, $w = w(x_1, \ldots, x_r) = w(n) \ldots w(2)w(1)$, kde $w(i) = x_k$ pro vhodné $k \in \{1, \ldots, r\}$. A dále $\gamma : \{1, \ldots, n\} \times X \to X$ bijekce.
O i řekneme, že je použité, pokud $w_i = w(i) \ldots w(2)w(1)$ je orámované. V opačném případě nazýváme i nové.
Naším úkolem je nalézt $a(1), a(2), \ldots, a(n) \in PT(X)$ taková, že $a(n) \ldots a(2)a(1) = s$, přičemž $a(i) = a(j)$ kdykoli $w(i) = w(j)$. Budeme postupně definovat $a(i) \in PT(X)$ a to tak, že $a_i = a(i) \ldots a(2)a(1) = \gamma(i, -)$ pro nová $i < n$.
Položme tedy $a(1) = \gamma(1, -)$.
Pokud je i použité, potom $w(i) \ldots w(i-j+2)w(i-j+1) = w(j) \ldots w(2)w(1)$. Proto $Im(a_{i-1}) \subseteq Im(a_{j-1})$ a $a(i) = a(j)$ je již na $Im(a_{i-1})$ definováno.
Pro i nové předpokládejme, že pro všechna nová $j < i$ platí $a_j = \gamma(j, -)$. $a(i)$ lze dodefinovat právě tehdy, když $Im(a_{i-1}) \cap Im(a_{j-1}) = \emptyset$ pro všechna j taková, že $w(i) = w(j)$. Stačí si uvědomit, že $w(k) \neq w(l) \Longrightarrow Im(a_k) \cap Im(a_l) = \emptyset$, tzn. především pro $w(i-1) \neq w(j-1)$ je $Im(a_{i-1}) \cap Im(a_{j-1}) = \emptyset$. Protože všechna $a(l)$ jsou prostá, lze z existence nejmenšího $k \in \mathbb{N}$ s vlastností $w(i-k) \neq w(j-k)$ (a to existuje, protože i nové) odvodit $Im(a_{i-1}) \cap Im(a_{j-1}) = \emptyset$, neboť $a(i-1) \ldots a(i-k+1) = a(j-1) \ldots a(j-k+1)$ je prostá transformace. Tedy $a(i)$ lze libovolně dodefinovat. My to učiníme tak, že $a_i = \gamma(i, -)$.
V posledním kroku, protože n je nové, lze dodefinovat $a(n)$ tak, že $a_n = s$. $\square$

Hypotéza. [D. M. Silberger – 1973]
Pro libovolnou množinu X a libovolné slovo w platí:
i) w je univerzální v $T(X)$ právě tehdy, když $\overline{w}$ je univerzální v $T(X)$,
ii) w je univerzální v $PT(X)$ právě tehdy, když $\overline{w}$ je univerzální v $PT(X)$.

Pro slova obshující dvě proměnné se podařila dokázat tato věta.

Věta 7. [K. Rother ... [13] – theorem 1]
Buď $w = w(x, y)$ pak následující dvě tvrzení jsou ekvivalentní
1) w je univerzální ve všech konečných $PT(X)$,
2) $\overline{w}$ je univerzální ve všech konečných $PT(X)$.

Autoři tuto větu dokázali s využitím věty 4 a očekávají, že stejnou metodou ji lze dokázat pro libovolné slovo.

Kapitola 4

Verbální úplnost pologrup a grup

Pokusme se dát odpověď na otázku, jak mohou vypadat pologrupy a grupy, v kterých jsou univerzální všechna slova.

Verbálně úplné pologrupy

O pologrupě $(S, \cdot)$ řekneme, že je *verbálně úplná* jestliže v S jsou univerzální všechna slova.

Lemma 1.
Pologrupa S je verbálně úplná právě tehdy, když jsou v S univerzální mocniny.
Důkaz:
$\Longrightarrow$: Zřejmé.
$\Longleftarrow$: Buď $w = w(x_1, \dots, x_r)$ libovolné slovo. Dosaďme do něj $x_i \mapsto x$ a dostaneme $w' = x^k$. Podle předpokladu je w' univerzální, a proto je univerzální i w. (Dle věty 2.1.) $\square$

Lemma 2.
Buď S pologrupa. Nechť $m = p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r} \in \mathbb{N}$, kde $p_1 < \dots < p_r$ jsou prvočísla, $\varepsilon_1, \dots, \varepsilon_r \in \mathbb{N}$ a označme pro jednoduchost $m_i = {p_i}^{\varepsilon_i}$. Podobně $n = p^\varepsilon$, kde p je prvočíslo a $\varepsilon \in \mathbb{N}$. Pak platí
i) x^m je univerzální v $S \Longleftrightarrow$ všechna slova x^{m_i} jsou univerzální v S,
ii) x^n je univerzální v $S \Longleftrightarrow x^p$ je univerzální v S.
Důkaz:
i) $\Longrightarrow$: Platí, neboť lze psát $x^m = (x^{\frac{m}{m_i}})^{m_i}$.
i) $\Longleftarrow$: Buď $s \in S$ libovolný prvek, pak postupně

$$s = s_1^{m_1}, s_1 = s_2^{m_2}, \dots, s_{r-1} = s_r^{m_r}.$$

Pak ale $s = s_r^m$.
ii) Zcela analogicky. $\square$

Spojením předchozích lemmat dostaneme charakterizaci verbálně úplných pologrup.

Věta 1.
Pologrupa S je verbálně úplná právě tehdy, když jsou v S univerzální slova x^p, kde p probíhá množinu všech prvočísel.

Jako příklad verbálně úplných pologrupy, nám poslouží pologrupy splňujíci identitu $x^2 = x$, tzv. bandy. Jsou to ale všechny? Nikoliv, známe další. Například $(\mathbb{Q}, +)$; $(\mathbb{Q}^+, +)$; $(\mathbb{R}^+, \cdot)$; $(\mathbb{R}^{1+}, \cdot)$ – reálná čísla větší než 1; $(\mathbb{C}, \cdot)$; $(\mathbb{C}^1, \cdot)$ – komplexní čísla jejichž absolutní hodnota je rovna 1. Všechny uvedené pologrupy jsou nekonečné. To není náhodou, neboť platí následující tvrzení.

Věta 2.
Každá konečná verbálně úplná pologrupa S je band.
Důkaz:
V S musí být univerzální všechny mocniny. Z konečnosti plyne, že všechna zobrazení $a \mapsto a^m$, pro $m \in \mathbb{N}$, jsou bijekcemi na S. Předpokládejme, že existuje $s \in S$ takové, že $s \neq s^2$. Protože $a \mapsto a^2$ je permutace konečné množiny S, musí existovat $n \in \mathbb{N}$ tak, že $s^{2^n} = s$. Pak ovšem platí:

$$(s^2)^{2^n-1} = s^{2^n+2^n-2} = s^{2^n} \cdot s^{2^n-2} = s \cdot s^{2^n-2} = s^{2^n-1}.$$

Předpokládali jsme však, že $s \neq s^2$ a tudíž $a \mapsto a^m$ pro $m = 2^n - 1$ není prosté a tedy ani surjektivní. Odtud plyne, že x^{2^n-1} není univerzální v S. Spor. Dokázali jsme, že $\forall\ s \in S$ platí $s = s^2$. $\square$

Verbálně úplné grupy

O grupě řekneme, že je *verbálně úplná*, pokud je netriviální a jsou v ní univerzální všechna neprázdná slova. Situace je nyní poněkud složitější. Lemma 2 platí v plném rozsahu, avšak lemma 1 pro grupy neplatí. Důkaz neprojde neboť, w' může být prázdné slovo. Například mocniny jsou univerzální v $(\mathbb{C}^*, \cdot)$, ale protože násobení na $\mathbb{C}$ je komutativní, nemůže být v $\mathbb{C}^*$ univerzální komutátor $[x, y] = x^{-1}y^{-1}xy$.

Snadno se vidí, že verbálně úplná grupa musí být nekonečná. V konečné grupě G totiž pro libovolný prvek g platí $g^{|G|} = 1$, proto slovo $x^{|G|}$ není univerzální v G. Obecněji lze říci, že ve verbálně úplné grupě neplatí žádná identita. Vzhledem k větě 2.3. platí, že libovolný netriviální kvocient verbálně úplné grupy je verbálně úplný. Tedy verbálně úplná grupa nemůže mít konečnou netriviální faktorgrupu. Ukážeme nyní příklad verbálně úplných grup.

Označme $S_\nu = S(X)$ pro nekonečnou množinu X kardinality $\aleph_\nu$. Dále

$$S_\nu^\tau = \{s \in S_\nu \mid |supp(s)| < \aleph_\tau\} \text{ pro } 0 \leq \tau \leq \nu + 1$$

$$A_\nu = \{s \in S_\nu^0 \mid s\,|_{supp(s)} \text{ sudá }\}.$$

Lze dokázat, že toto jsou jediné normalní podgrupy grupy S_ν. Označme $H_\nu^\tau = S_\nu^{\tau+1}/S_\nu^\tau$. (Jsou to jednoduché grupy.)

Věta 3. [M. Droste [2] – theorem 5]
Pro $0 < \tau \leq \nu$ jsou H_ν^τ verbálně úplné grupy.
Důkaz:
Buď $w = w(x_1, \ldots, x_r)$ libovolné neprázdné slovo. Ukážeme o něm, že je univerzální v H_ν^τ. Pro $s \in S_\nu^{\tau+1}$ existuje s' takové, že $s' \in sH_\nu^\tau$ a $\forall\ 2 \leq n \in \mathbb{N}_\infty : \widetilde{s'}(n) = 0$ nebo $\widetilde{s'}(n) = \aleph_\tau$. Pokud budeme umět reprezentovat pro každé $m \in \mathbb{N}_\infty$ prvek $a \in S_\nu^{\tau+1}$ vlastností $\widetilde{a}(m) = \aleph_\tau, \widetilde{a}(n) = 0$ pro $n \neq m$, $n \in \mathbb{N}_\infty$ máme dokázáno celé tvrzení.
Buď tedy pro pevné m dáno $a \in S_\nu^{\tau+1}$ popsaných vlastností. Vezměme grupu G (její existenci prodiskutujeme v následujícím lemmatu) těchto vlastností: $|G| = \aleph_\tau$ a existují $g, g_1, \ldots, g_r \in G$ takové, že $g = w(g_1, \ldots, g_r)$ je řádu m. Uvažme nyní Cayleyho reprezentaci grupy G, tedy

$$\alpha : G \hookrightarrow S(G) \cong S_\tau \subseteq S_\nu^{\tau+1}.$$

Potom platí $\alpha(g)(h) = gh$ pro libovolné $h \in G$. Vzhledem k tomu, že řád g je m, je $\alpha(g)$ permutace pro niž $\widetilde{\alpha(g)} = \widetilde{a}$. Existuje tedy $c \in S_\nu^{\tau+1}$ tak, že $a = c^{-1}\alpha(g)c$. Snadno se již ověří, že

$$\begin{aligned} a &= c^{-1}\alpha(g)\,c \\ &= c^{-1}\alpha(w(g_1, \ldots, g_r))\,c \\ &= c^{-1}w(\alpha(g_1), \ldots, \alpha(g_r))\,c \\ &= w(c^{-1}\alpha(g_1)c, \ldots, c^{-1}\alpha(g_r)c) \end{aligned}$$

a důkaz je dokončen. □

Lemma 3.
Pro libovolné slovo $w = w(x_1, \ldots, x_r)$ a libovolné $m \in \mathbb{N}_\infty$ existuje grupa G mohutnosti $\aleph_\tau$ a v ní prvky $g, g_1, \ldots, g_r$ takové, že $w(g_1, \ldots, g_r) = g$ je řádu m.
Důkaz:
Nejdříve poznamenejme, že pro $m = \aleph_0$ je tvrzení zřejmé: stačí vzít volnou grupu a v ní

libovolné prvky různé od 1. Pro $m \in \mathbb{N}$ stačí dokázat pro grupu mohutnosti $\aleph_0$, neboť z ní lze získat, vynásobením vhodnou grupou, grupu libovolné mohutnosti. Položme

$$G = \langle\, x_0, x_1, \ldots, x_r \mid w(x_1, \ldots, x_r)^m \,\rangle.$$

Pokud w není mocninou nějakého slova a je cyklicky redukováno, pak podle [10] – theorem 5.2. (resp. [9]) je $w(x_1, \ldots, x_r)$ prvek řádu m v G. Pokud w takové není, lze stejnou úvahu provést pro slovo, které je cyklicky redukovaným tvarem slova u, kde slovo u není mocninou a pro něž $u^n = w$. Pak u je prvek řádu $n \cdot m$, a proto opět $w(x_1, \ldots, x_r)$ je prvek řádu m v G. $\square$

Na tomto místě bychom se měli zmínit, že nekonečné permutační grupy nejsou verbálně úplné, protože v nich nejsou univerzální mocniny. Platí však následující věta.

Věta 4. [Lyndon [11]]
Slovo w není univerzální v nekonečné grupě $S(X)$ právě tehdy, když lze psát ve tvaru $w = v^n$, kde $1 < n \in \mathbb{N}$.

Kapitola 5

Univerzální slova tvaru $x^n y^m$

Vraťme se nyní opět ke grupě permutací a monoidům transformací. V následujícím ukážeme některá tvrzení, která platí pro nejjednoduší netriviální slova, totiž slova tvaru $x^n y^m$. Některá tvrzení lze zobnecnit díky větě 2.1. Protože takové důsledky jsou zřejmé, budeme se zabývat pouze slovy $x^n y^m$.

Charakterizace univerzálních slov v transformacích

Pro prvočíslo p označme $\mu(p)$ nejmenší společný násobek čísel $1, 2, 3, \ldots, p$. Pro libovolné $1 < n \in \mathbb{N}$ označme $\pi(n)$ nejmenší prvočíslo dělící n a rozšiřme definici μ takto $\mu(n) = \mu(\pi(n))$.

Věta 1. [A. Ehrenfeucht a D. M. Silberger [5] – 1.1., D. M. Silberger [15] – 1.1.]
Nechť $1 < m, n \in \mathbb{N}$ a $w = x^n y^m$. Následující tvrzení jsou ekvivalentní:
1) $\mu(n) \nmid m$ a $\mu(m) \nmid n$,
2) slovo w je univerzální ve všech $S(X)$,
3) slovo w je univerzální ve všech $T(X)$,
4) slovo w je univerzální ve všech $PT(X)$,
5) slovo w je univerzální ve všech konečných $S(X)$,
6) slovo w je univerzální ve všech konečných $T(X)$,
7) slovo w je univerzální ve všech konečných $PT(X)$.
Důkaz:
Provedeme v několika krocích.
2) $\Longleftrightarrow$ 5) plyne z Lemmatu 1 , kde ukážeme, že všechna slova tvaru $x^n y^m$ jsou univerzální v nekonečných $S(X)$.
Podobně z Lemmatu 2 dostaneme 3) $\Longleftrightarrow$ 6) , 4) $\Longleftrightarrow$ 7).
Implikace 7) $\Longrightarrow$ 6) $\Longrightarrow$ 5) platí obecně pro libovolné slovo w (věty 3.1. a 3.2.).
5) $\Longrightarrow$ 7) je důsledkem Lemmatu 4.
Konečně ekvivalence 1) $\Longleftrightarrow$ 5) je obsahem lemmatu 5.

Lemma 1. [D. M. Silberger [16] – theorem 1]
Libovolné slovo $x^n y^m$ je univerzální v $S(X)$, kde X je nekonečná.
Důkaz:
Uvedeme zde trochu jiný důkaz. Buď $s \in S(X)$ rozloženo na disjunktní cykly. Ty jsou buď konečné, nebo nekonečné. Všechny rozepišme tímto způsobem:

$$(1,2)(3,4)\dots(2k-1,2k) \circ (2,3)(4,5)\dots(2k-2,2k-1)$$

pro sudé cykly respektive

$$(1,2)(3,4)\dots(2k-1,2k) \circ (2,3)(4,5)\dots(2k-2,2k-1)(2k,2k+1)$$

pro liché, respektive

$$(1,2)(3,4)(5,6)\dots \circ (2,3)(4,5)(6,7)\dots$$

pro nekonečné cykly.
Tímto způsobem můžeme psát $s = a \circ b$, kde $a, b \in S(X)$ se skládá z cyklů délky 2. Pokud by těchto cyklů bylo jen konečně mnoho, pak $supp(s)$ je konečná a existuje tedy $c \in S(X)$ sestávající z nekonečně mnoha cyklů délky 2 tak, že můžeme psát $s = ac \circ cb$. Tedy $s = a' \circ b'$, kde a', b' obsahuje nekonečně mnoho cyklů délky 2. Ty združíme do skupin po n respektive m a pomocí rovnosti

$$(1,l+1)(2,l+2)\dots(l,2l) = (1,2,3,\dots,2l)^l$$

odmocníme. Tím dostaneme a'', b'' pro které platí $(a'')^n(b'')^m = s$. $\square$

Lemma 2.
Libovolné slovo $x^n y^m$ je univerzální v $T(X)$, $PT(X)$, kde X je nekonečná.
Důkaz:
Lemma je jednoduchým důsledkem věty 3.6. Přesto ukažme jak lze psát libovolný prvek $s \in PT(\mathbb{N})$ ve tvaru $a^n b^m$. Pro dostatečně velké $k \in \mathbb{N}$ ($k^m \geq n$) položme

$$\begin{array}{lcll} b(i) & = & ki & \text{pro } i \in \mathbb{N}, \\ a(k^m i - j) & = & k^m i - j - 1 & \text{pro } j \in \{0,1,\dots,n-2\}, \\ a(k^m i - (n-1)) & = & s(i). & \end{array}$$ $\square$

Lemma 3.
Je-li $x^n y^m$ univerzální v $S(k)$, pak reprezentuje libovolný prvek $s \in PT(l)$, pro který platí $|Im(s)| = k$.
Důkaz:
Buď $s \in PT(X)$ libovolné s vlastností $|Im(s)| = k$ (přičemž $|X| = l$). Pro každý prvek $f \in Im(s) \subseteq X$ zvolme jeden vzor. Množinu těchto vzorů označme RD, $s' = s\,|_{RD}$, přičemž

$|RD| = |Im(s)| = k$. Pokud se nám podaří s' napsat ve tvaru $a^n b_0^m$, kde $a \in PT(l)$, $b_0 \in S(RD)$, máme tvrzení dokázáno, neboť b_0 pak snadno dodefinujeme na $b \in PT(l)$ tak, aby $s = a^n b^m$. ($b(f) = b_0(e)$, kde $e \in RD$ a $s(f) = s(e)$.)

Tedy $s' : RD \to X$ prosté a označme pro jednoduchost $Im(s') = Im(s)$ jako Im. Protože $|Im \setminus RD| = |RD \setminus Im|$, existuje bijekce $\iota_0 : Im \setminus RD \to RD \setminus Im$. Označme nyní $s'' = \iota s'$, kde $\iota : Im \to RD$ je bijekce definována takto: $\iota|_{Im \cap RD} = id_{Im \cap RD}$, $\iota|_{Im \setminus RD} = \iota_0$. Protože $s'' \in S(RD)$, existují dle předpokladu $a_0, b_0 \in S(RD)$ tak, že $s'' = a_0^n b_0^m$.

Nyní definujme $a_1 : RD \to Im$ vztahem $a_1 = \iota^{-1} a_0$. Dále definujme $a \in PT(l)$ takto: $a|_{RD} = a_1$, $a|_{Im \setminus RD} = a_1 \iota_0 = a_1 \iota|_{Im \setminus RD}$. Potom $a : Im \cup RD \to Im$. Indukcí lze snadno dokázat $a^n|_{RD} = \iota^{-1} a_0^n$, Odkud dostáváme $a^n b_0^m = \iota^{-1} a_0^n b_0^m = \iota^{-1} s'' = \iota^{-1} \iota s' = id_{Im} s' = s'$. □

Lemma 4.
Je-li $x^n y^m$ univerzální v $S(k)$, pro všechna $k \leq l \in \mathbb{N}$, pak je univerzální v $PT(l)$.
Důkaz:
Lemma je jednoduchým důsledkem předchozího lemmatu 3. □

Lemma 5.
Slovo $w = x^n y^m$ pro $1 < m, n \in \mathbb{N}$ je univerzální ve všech konečných $S(X)$ právě tehdy, když $\mu(n) \nmid m$ a $\mu(m) \nmid n$.
Důkaz:
$\Longrightarrow$: Nechť podmínka neplatí. Označme $p = \pi(m)$ a předpokládejme, že $\mu(m) = \mu(p) \mid n$. Potom $\forall\, a \in S(p)$ platí $a^{\mu(p)} = id$ a tedy $a^n = id$. Má-li být slovo $x^n y^m$ univerzální v $S(p)$, musí být univerzální slovo y^m. Avšak $p \mid m$ a proto nelze reprezentovat cyklus délky p. Vzhledem k tomu, že v konečných $S(X)$ je w univerzální právě tehdy, když je univerzální $\overline{w}$ (věta 2.7.) je tato implikace dokázána.
$\Longleftarrow$: Stačí dokázat, že umíme psát ve tvaru $a^n b^m$ libovolný cyklus délky k v $S(k)$. Pokud by n, m byla sudá, pak $\mu(n) = \mu(m) = 2$ a podmínka není splněna. Opět vzhledem k větě 2.7., můžeme předpokládat, že n je liché. Druhá podmínka je potom splněna, neboť $2 \mid \mu(m)$. Označme $p = \pi(n)$ a platí $\mu(p) \nmid m$. Poznamenejme, že pro $k < p$ lze brát $b = id$ a a vhodný cyklus délky k. Dále tedy $k \geq p$ a rozlišme dva případy: $p \nmid m$ a $p \mid m$.
i) $p \nmid m$. Označme $d = \lfloor \frac{k}{p} \rfloor$ a položme

$$b^m = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \ldots (\ldots, dp)$$

$$a^n = (1, dp+1)(2, dp+2) \ldots (k - dp, k) \circ (p, p+1)(2p, 2p+1) \ldots ((d-1)p, (d-1)p+1).$$

Potom $a^n b^m$ je cyklus délky k, přičemž a^n, b^m lze odmocnit, neboť $p \nmid m$ a n liché.
ii) $p \mid m$. Pak existuje prvočíslo q a $0 \leq \eta < \varepsilon \in \mathbb{N}_0$ tak, že

$$q^{\varepsilon} < p, \quad q^{\varepsilon} \nmid m, \quad n.s.d.(q^{\varepsilon}, m) = q^{\eta}.$$

Označme $d = \lfloor \frac{k}{q^{\varepsilon}} \rfloor$ a položme

$$b = (1, \ldots, q^{\varepsilon})(q^{\varepsilon} + 1, \ldots, 2q^{\varepsilon}) \ldots (\ldots, dq^{\varepsilon}).$$

Pak b^m se skládá z dq^{η} cyklů délky $q^{\varepsilon - \eta}$. Pišme dále raději

$$b^m = (1, 2, \ldots, \overline{q})(\overline{q} + 1, \overline{q} + 2, \ldots, 2\overline{q}) \ldots (\ldots, \overline{d}\,\overline{q})$$

kde $\overline{d} = dq^{\eta}$, $\overline{q} = q^{\varepsilon - \eta}$ a víme, že umíme odmocnit. Nyní položme

$$a^n = (\overline{q}, \overline{q} + 1)(2\overline{q}, 2\overline{q} + 1) \ldots ((\overline{d} - 1)\overline{q}, (\overline{d} - 1)\overline{q} + 1) \circ (\overline{d}\,\overline{q}, dq^{\varepsilon} + 1, dq^{\varepsilon} + 2, \ldots, k).$$

Pak a^n lze odmocnit, neboť jsou to cykly délky 2 (n je liché) a poslední cyklus je nejvýše délky q^{ε} ($q^{\varepsilon} < p$, proto je jeho délka nesoudělná s n).Tím je důkaz dokončen. □

Předchozí chartakterizační větu lze taktéž dokázat pro prosté parciální transformace.

Věta 2.
Nechť $1 < m, n \in \mathbb{N}$ a $w = x^n y^m$. Následující tvrzení jsou ekvivalentní:
5) slovo w je univerzální ve všech konečných $S(X)$,
8) slovo w je univerzální ve všech konečných $I(X)$,
9) slovo w je univerzální ve všech $I(X)$.
Důkaz:
8) $\Longleftrightarrow$ 9) plyne z faktu, že libovolné slovo $x^n y^m$ je univerzální v nekonečných $I(X)$, což dokážeme v lemmatu 6.
8) $\Longrightarrow$ 5) Plyne z věty 3.3.
5) $\Longrightarrow$ 8) Každý prvek v $I(k)$ se rozpadá na disjunktní cykly a hady. Stačí tedy dokázat, že hada délky k umíme vyjádřit ve tvaru $a^n b^m$ v $I(k)$. Pokud bychom uměli cyklus délky k psát ve tvaru $a^n b^m$, kde a nebo b má pevný bod, potom vypuštěním tohoto bodu bude $a^n b^m$ had délky k. Stačí tedy sledovat důkaz lemmatu 5 a zjistíme, že každé zkonstruované $a^n b^m$ má nějaký pevný bod. Opravdu.
V případě kdy $k < p$ je $b = id$ a máme pevný bod.
Když $k \geq p$, pak postupně
i) $b(k) = k$ pokud $p \nmid k$ a
$a(1) = 1$ pokud $p \mid k$,
ii) $a(1) = 1$. □

Lemma 6.
Libovolné slovo $x^n y^m$ je univerzální v $I(X)$, kde X je nekonečná.
Důkaz:
Stačí, když ukážeme, že $x^n y^m$ je univerzální v $I(\mathbb{N})$.

Buď $s \in I(\mathbb{N})$ libovolné. Uvažme rostoucí posloupnost sudých čísel $(c_i)_{i\in\mathbb{N}}$ splňující $c_{2i-1}, c_{2i} > \max\{i, s(i)\}$. (Můžeme například volit $c_1 = 2(1+s(1)), c_{2i-1} = 2(c_{2i-2} + i + s(i)), c_{2i} = c_{2i-1} + 2$.)

Definujme nyní $a, b \in I(\mathbb{N})$ takto,

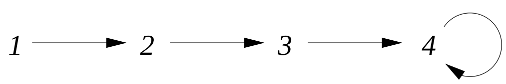
$$a(i) = c_{2i}, \qquad b(j) = \begin{cases} c_{2s^{-1}(j)}, & j \in Im(s) \\ c_{2j-1}, & j \notin Im(s). \end{cases}$$

Potom $b^{-1}a(i) = b^{-1}(c_{2i}) = j$ pokud $i = s^{-1}(j)$, jinak není $b^{-1}a(i)$ definované, tzn. $b^{-1}a = s$. Protože a, b jsou monotóní, neobsahují cykly, a protože $Dom(a) = Dom(b) = \mathbb{N}$, neobsahují taktéž konečné a nezačínající hady. Vzhledem k tomu, že $Im(a) \cup Im(b) \subseteq 2\mathbb{N}$, sestává a (resp. b) z nekonečně mnoha nekončících hadů, a lze jej tedy psát ve tvaru ${a_0}^m$ (resp. ${b_0}^n$). Dostáváme tedy $({b_0}^{-1})^n {a_0}^m = b^{-1}a = s$. $\square$

Poznámka.
Zmiňme se nyní o tom, jakým způsobem věty 1 a 2 dokázali autoři v [5] a [15]. V [5] dokázali ekvivalence 1) $\Longleftrightarrow$ 5) $\Longleftrightarrow$ 6), přičemž od našeho postupu se odchýlili v tom, že dokazovali implikaci 1) $\Longrightarrow$ 6) přímo. Pro libovolné $s \in T(X)$ nalezli $a, b \in T(X)$ následujících vlastností: $s = a^n b^m$, kde n sudé a m liché, $b \in S(k)$ a $a \in T(k)$ splňující $\forall\, e \in X\, \exists\, l \in \mathbb{N} : a(e) = a^{l+1}(e)$. Naproti tomu v [15] byl důkaz veden jiným způsobem. Zde byla dokázána implikace 1) $\Longrightarrow$ 8) a s využitím důsledku 3.5. implikace 8) $\Longrightarrow$ 7). Zbylé se liší jen drobnostmi, např. Lemma 1 není použito, ale pouze vyjádřen nekonečný had ve tvaru $a^n b^m$. Náš důkaz je tedy jiný především lemmatem 3.

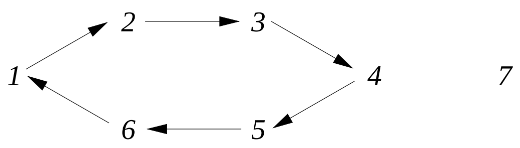
Je přirozené se ptát zda neplatí nějaké zobecnění lemmatu 3. Negativní odpovědi dávají následující příklady.

Příklady.
1) Slovo $x^6 y^5 x^6$ je univerzální ve všech grupách a tedy i ve všech permutačních grupách. Lze však ukázat, že není univerzální v $T(4)$, nelze jím totiž reprezentovat následující transformaci.



Kdyby se dala tato transformace psát ve tvaru $a^6b^5a^6$, rozliší se dva případy. V případě kdy a je permutace lze ji taktéž psát ve tvaru $a^{12}(a^{-6}ba^6)^5$, kde $a^{12} = id$, což nelze. V případě kdy a není permutace se ukáže, že $|Im(a^6)| \leq 2$.

2) Slovo $x^{\mu(5)}y^3$ je univerzální v $S(7)$ a není univerzální v $PT(7)$, neboť nereprezentuje v $PT(7)$ následující parciální transformaci.



Jedna otázka však zůstává nezodpovězena. Existuje slovo $w = x^n y^m$, které je univerzální v $S(k)$ a není univerzální v $T(k)$?

Asymptotická univerzalita

V předešlém jsme charakterizovali slova tvaru $x^n y^m$, která jsou univerzální ve všech $S(k)$. Podle důkazu zmíněné věty víme, že slovo x^6y^3 není univerzální v $S(3)$. Co lze ale říci o univerzalitě tohoto slova v ostatních $S(k)$? Odpověď nám dájí následující příklady.

Příklady.
1) x^6y^3 není univerzální v $S(4)$.
Důkaz:
Předpokládejme, že existují $a, b \in S(4)$ takové, že $a^6b^3 = (1, 2, 3)$. Nutně musí být b sudá permutace. Protože cyklus délky 3 nelze psát ve tvaru c^3, je $a^6, b^3 \neq id$. Proto je a cyklus délky 4 a b se skládá ze dvou cyklů délky 2. Odtud

$$a^6, b^3 \in V = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

a tedy i $(1, 2, 3) \in V$, neboť V je podgrupa $S(4)$. Spor.

2) x^6y^3 je univerzální v $S(k)$ pro všechna $k \geq 5$.
Důkaz:
Buď $s \in S(k)$ libovolný a označme $|s|$ počet cyklů v rozkladu s na disjunktní cykly. Rozlišme několik případů.

I) $|s| = 1$. a) Pokud tento cyklus má délku, která není dělitelná 3, pak lze snadno psát $s = b^3$ pro vhodné $b \in S(k)$.
b) Cyklus délky 3 umíme v tomto tvaru psát:

$$(5, 2, 3, 4, 1)^6 \circ ((1, 5)(3, 4))^3 = (1, 2, 3).$$

c) Zbývá rozepsat

$$(1, 2, \ldots, 3l) = (1, 3l-1, 2, 3l)^6 \circ (2, \ldots, 3l-2, 3l),$$

přičemž poslední cyklus je délky $3l-2$ a lze tedy psát ve tvaru b^3 pro vhodné $b \in S(k)$.

II) $|s| \geq 2$ liché. a) Pokud některý cyklus z rozkladu s není délky 3, pak jej lze rozložit dle bodu Ia nebo Ic a přejít k $|s|$ sudé.
b)Všechny cykly jsou délky 3, pak upravíme 3 z nich

$$(1, 2, 3)(4, 5, 6)(7, 8, 9) = (1, 8, 4, 3, 7, 6, 2, 9, 5)^6$$

a přejdeme k $|s|$ sudé.

III) $|s| \geq 2$ sudé. Každý cyklus z rozkladu budeme psát ve tvaru buď

$$(1, 2, \ldots, l) = (1, 2) \circ (2, 3, \ldots, l)$$

nebo

$$(1, 2, \ldots, l) = (1, 3) \circ (1, 2)(3, 4, \ldots, l)$$

a to tak, aby napravo zůstal cyklus jehož délka není dělitelná 3. Tím získáme rozklad $s = a \circ b$, kde $a = x^6$ a $b = y^3$ má řešení, neboť a sestává ze sudého počtu cyklů délky 2 a b z cyklů jejichž délka není dělitelná 3.

Podobně bychom chtěli vědět, zda pro libovolné $x^n y^m$ existuje $K(n, m) \in \mathbb{N}$ takové, že $x^n y^m$ je univerzální v $S(k)$ pro $k \geq K(n, m)$. Odpověť nalezneme v následující větě. Pro n, m nenulová celá čísla označme $\rho(n, m) \in \mathbb{N}$ součin prvočísel, která dělí $n \cdot m$, s přihlédnutím ke konvenci $\rho(n, m) = 1$ pokud $n, m \in \{-1, 1\}$.

Věta 3. [M. Droste [3]]
1) Buď n, m celá nenulová čísla, pak $x^n y^m$ je univerzální v $A(k)$ pro všechna $k \geq 4 \cdot \rho(n, m) + 1$.
2) Buď n, m nenulová, ne obě sudá celá čísla. Pak $x^n y^m$ je univerzální v $S(k)$ pro všechna $k \geq 4 \cdot \rho(n, m)$.
Důkaz:
Pouze naznačíme důkaz 1. části. Pro $\rho(n, m) = 1$ zřejmé. Pro $\rho(n, m) > 1$ nám podmínka $k \geq 4 \cdot \rho(n, m) + 1$ zaručuje existenci $l \in \mathbb{N}$ následujících vlastností:

$$\begin{array}{ll} (i) & \lfloor \frac{3}{4} k \rfloor \leq l \leq k-2 \\ (ii) & 2 \nmid l \\ (iii) & n.s.d.(l, n) = n.s.d.(l, m) = 1 \end{array}$$

Pro takové l a libovolný prvek $s \in A(k)$ pak podle [1] existují $a, b \in S(k)$ cykly délky l takové, že $a \circ b = s$. Navíc podmínka (ii) dá $a, b \in A(k)$ a podmínka (iii) umožní odmocnění.

Podobným způsobem se dokáže i 2. část, opět pomocí výsledků [1]. $\square$

Důsledek 4. [M. Droste [3]]
1) Buď n, m celá nenulová čísla, X nekonečná množina. Pak $x^n y^m$ je univerzální v $A(X)$.
2) Buď n, m nenulová, ne obě sudá celá čísla, X nekonečná množina. Pak $x^n y^m$ je univerzální v $S^0(X)$.

Na základě předchozí věty jsme schopni dokázat analogické tvrzení pro monoidy transformací.

Věta 5.
Buď $n, m \in \mathbb{N}$, ne obě sudá. Pak $x^n y^m$ je univerzální v $PT(l)$ pro každé $l \geq K = 8n \cdot \rho(n, m)$.
Důkaz:
Využijeme věty 3 a lemmatu 3 této kapitoly. Buď $l \geq K$, $s \in PT(l)$ a označme $k = |Im(s)|$. Pokud $k \geq 4 \cdot \rho(n, m)$, pak $x^n y^m$ je univerzální v $S(k)$ a tedy reprezentuje prvek $s \in PT(l)$ dle lemmatu 3.
Pokud $k < 4 \cdot \rho(n, m)$, budeme postupovat stejně jako v důkaze lemmatu 3. Označíme RD množinu reprezenativních vzorů a $s' = s|_{RD}$ prostou parciální transformaci. Naším cílem bude rozepsat $s' = a^n \circ id_{RD}$, kde $a \in S(l)$, což učiníme následujícím způsobem. Nejdříve s' doplníme na $s'' \in S(2k)$ (to lze neboť $s' \in I(2k)$). Nyní ke každému cyklu z s'' přidáme $n - 1$ cyklů stejné délky. Tím obdržíme permutaci, kterou lze psát ve tvaru a^n a protože $k < 4 \cdot \rho(n, m)$ je $2k \cdot n < K \leq l$ a tedy $a \in S(l)$. Transformaci $b \in PT(l)$ zkonstruujeme způsobem z lemmatu 3. $\square$

Nevíme, zda platí stejné tvrzení pro prosté parciální transformace. Způsobem, kterým jsme dokázali předchozí větu se nám dokázat nepodaří, neboť v důkaze lemmatu 3 nebylo zkonstruované a v rozkladu $s = a^n b^m$ prosté.

Literatura

[1] Bertram, E.A., *Even permutations as the product of two conjugate cycles,* J. Combinatorial Theory A *12* (1972), 368–380.

[2] Droste, M., *Classes of universal words for the infinite symmetric groups,* Algebra Universalis *20* (1985), 205–216.

[3] Droste, M., *On the universality of words for the alterning groups,* Proceedings Amer. Math. Soc. *96* (1986), 18–22.

[4] Ehrenfeucht, A., Fajtlowicz, S., Malitz, J. and Mycielski, J., *Some problems on the universality of words in groups,* Algebra Universalis *11* (1980), 261–263.

[5] Ehrenfeucht, A. and Silberger, D.M., *Universal terms of the form $B^n A^m$,* Algebra Universalis *10* (1980), 96–116.

[6] Grätzer, G., *Universal Algebra,* Springer-Verlag (1979).

[7] Howie, J.M., *An Introduction to Semigroup Theory,* Academic Press Inc., London (1976).

[8] Isbell, J.R., *On the problem of universal terms,* Bull. de L'Academie Polonaise des Sciences XIV (1966), 593–595.

[9] Karrass, A., Magnus, W. and Solitar, D., *Elements of finite order in groups with a single defining relation,* Comm. Pure Appl. Math. *13* (1960), 57–66.

[10] Lyndon, R.C. and Schupp, P.E., *Combinatorial Group Theory,* Springer-Verlag (1977) – ruský překlad: Mir, Moskva (1980).

[11] Lyndon, R.C., *Words and infinite permutations, Mots (ed. M. Lothaire),* Hermes, Paris (1990) [ISBN 2-86601-206-2], 143–152.

[12] Ore, O., *Some remarks on commutators,* Proceedings Amer. Math. Soc. *2* (1951), 307–314.

[13] Rother, K., Silberger, D.M. and Wilson, M.E., *The reverse spelling of an FPrt–universal word in two letters,* Algebra Universalis *36* (1996), 202–221.

[14] Silberger, D.M., *When is a term point universal?* Algebra Universalis *10* (1980), 135–154.

[15] Silberger, D.M., *B^nA^m is universal iff point universal,* Algebra Universalis *12* (1981), 335–342.

[16] Silberger, D.M., *Are primitive words universal for infinite symmetric groups?* Algebra Universalis *16* (1983), 253–254.